IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

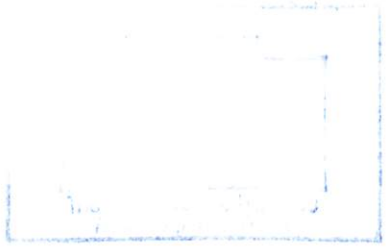
UNITED STATES OF AMERICA	)	
	)	
v.	)	No. 1:16-CR-313
	)	
JUSTIN GRAY LIVERMAN,	)	
(a/k/a "D3F4ULT")	)	
	)	
Defendant.	)	

STATEMENT OF FACTS

The United States and the defendant, JUSTIN GRAY LIVERMAN, a/k/a "D3F4ULT," agree that the following facts are true and correct, and that had this matter proceeded to trial, the United States would have proven them beyond a reasonable doubt with admissible and credible evidence:

1. From at least in or around November 2015 to in or around February 2016, defendant agreed and conspired with others to, among other things, obtain unauthorized access to U.S. government officials' online accounts and government computer databases, and conduct harassing telephone campaigns of victims who were senior U.S. government employees. Defendant's co-conspirators labeled themselves with the group moniker "Crackas with Attitude," or CWA.

2. During the conspiracy, defendant used several pseudonymous online accounts – which he created and controlled – to communicate with co-conspirators and publicly harass victims, among other things, including: (a) Twitter accounts @_D3F4ULT, @BASHTIEN_, and @SH1N0D4; (b) Jabber messaging account d3f4ult@jabber.lqdn.fr; and (c) Facebook and online accounts under the alias "Joseph Markowicz." In their communications, defendant and his co-



conspirators frequently used anonymizing programs such as virtual private networks, encrypted chat programs, and the encrypted Tor browser, to conceal their true identities and locations.

3. At all times during the conspiracy, defendant resided in North Carolina, although at times he falsely represented to co-conspirators that he was located in Florida or elsewhere. Defendant's co-conspirators were located in the United States and the United Kingdom, and included individuals who used the online monikers "CRACKA," "DERP," and "CUBED," and included a co-conspirator who used the Twitter account @INCURSIOSUBTER. CRACKA was the leader of CWA and resided in the United Kingdom.

4. In total, the conspiracy targeted more than 10 victims and caused more than $1.5 million in actual losses to victims, including service providers. The loss amount attributable to the defendant for his role in the conspiracy was at least $95,000. In the course of the conspiracy, defendant created and saved a computer file that he titled "cwa_targets." This file listed approximately 15 victims' names and their corresponding job titles, the majority of whom were senior U.S. government officials, and some of whom were residents of the Eastern District of Virginia.

Victim 1

5. In or around October 2015, defendant and co-conspirator CRACKA exchanged compliments online about the other's purported hacking exploits that were publicized on Twitter. In particular, defendant congratulated CRACKA in a private Twitter message for successfully gaining unauthorized access into Victim 1's online account, stating, "[Victim 1] got bent lol." At the time, Victim 1 was a senior U.S. government official who worked and resided in the Eastern District of Virginia. In the same conversation, defendant cautioned CRACKA to "stay safe and dban" – or erase evidence from – any computer drive he didn't need.

Victim 2

6. In or around November 2015, defendant and other co-conspirators agreed to target Victim 2 in a hacking and phone-harassment scheme. At the time, Victim 2 was a senior U.S. government official who worked for a federal law enforcement agency.

7. Specifically, on or about November 1, 2015, co-conspirator CRACKA informed defendant via Jabber's instant messaging function that CRACKA had gained unauthorized access to Victim 2's account with Internet service provider Comcast. Defendant replied to CRACKA, "plz jack all [Victim 2's] shit haha." Defendant further suggested that CRACKA hack into Victim 2's government email account, stating: "if you could get into [Victim 2's] [U.S. Government Agency] acc im sure it would yield"; "how hard u think itll be to get into [Victim 2's] [U.S. Government Agency] email acc?"; and it "would be nice" to gain access to Victim 2's government account. Later that day, defendant posted on his pseudonymous Facebook and Twitter accounts a screenshot of a document unlawfully obtained from Victim 2's online Comcast account.

8. On or about November 2, 2015, co-conspirator CRACKA provided defendant with Victim 2's cellphone number, which CRACKA had unlawfully obtained from Victim 2's online accounts. Defendant, in a Jabber chat with CRACKA, stated that he would "phonebomb" Victim 2 if the phone number was legitimate. Later that day, defendant dialed Victim 2's phone number and confirmed that it belonged to the victim. Defendant then paid an online service to automatically dial Victim 2's phone number once an hour, for 30 days, and leave a threatening recorded message. Two days later, defendant told CRACKA in a Jabber chat that he had "been phone bombing [Victim 2's phone] for 2 days," and that Victim 2 had received approximately "50 voicemails already."

9. On or about November 2, 2015, defendant used a temporary email service to send the following text messages to Victim 2's cellphone:

> Listen here you fucking boomer, we will destroy your reputation.
>
> Just like [Victim 1 and another senior U.S. government official]… I guess you couldn't handle us jacking your Comcast ISP accounts too many times so you actually canceled your account! And telling me to "watch my back" wasn't a good idea lol How is your slut wife [spouse first name]? We will keep a close eye on your family, especially your son!

At the end of the text message, defendant linked to a photograph of Victim 2's son that co-conspirator CRACKA unlawfully obtained from Victim 2's online account and sent to defendant. Defendant sent Victim 2 the above harassing messages multiple times.

10. On or about November 2, 2015, defendant wrote a note to himself on his computer that stated in part: "fucking golden . . . . jacked [Victim 2's] comcast isp account, got [Victim 2's] 200 contact list, found [Victim 2's] cell, spammed it via email to sms and now phone bombing [Victim 2]." On or about December 10, 2015, defendant also informed co-conspirator CRACKA via Jabber that as a result of defendant's "phonebombing" campaign, Victim 2's cellphone was flooded with "720 voicemail threats" and approximately 1,000 text messages depicting a lewd image of a man.

11. On or about November 2, 2015, defendant told co-conspirator CRACKA via Jabber that he wanted to post a Facebook message that solicited text messages and calls to Victim 2's cellphone number. Defendant then publicly posted Victim 2's cellphone number on his pseudonymous Facebook and Twitter accounts and wrote: "This line will be active for only 24hrs, so call/sms it if you want to talk to me… i also accept sexy nudes lol."

12. On or about November 4, 2015, defendant stated to co-conspirator CRACKA in a Jabber chat, "if we could get [Victim 2] swatted that would be amazing." By "swatted"

defendant was referring to the crime of placing hoax calls to an emergency service, such as a police department, to falsely report that an imminent or ongoing critical incident was occurring, for the purpose of eliciting a tactical police response to the location of the swatting victim.

13. On or about November 4, 2015, co-conspirator CRACKA informed defendant that he had used Victim 2's official credentials to obtain unauthorized access to the Law Enforcement Enterprise Portal ("LEEP"). LEEP is a U.S. government computer system that provides law enforcement agencies, intelligence groups, and criminal justice entities with access to resources such as the Joint Automated Booking System ("JABS"). Defendant asked CRACKA what information LEEP contained, querying "anything good?!" CRACKA responded, "every law enforcement info. fucking shaking." Defendant then asked CRACKA if he could search LEEP by city and stated that there were "many officers info in miami i would love." Defendant reiterated to CRACKA, "i would love a list of officers in miami ;)." Shortly thereafter and per defendant's request, CRACKA sent defendant a list of information CRACKA had obtained through Victim 2's LEEP account – including names, phone numbers, and email addresses – relating to more than 80 police officers and law enforcement employees in the Miami area. On or about January 21, 2016, defendant uploaded this information to publicly accessible websites.

Victim 3 and Victim 3's Spouse

14. In or around December 2015, defendant and other co-conspirators agreed – at defendant's urging – to target Victim 3 and Victim 3's spouse in their hacking and phone-harassment scheme. At the time, Victim 3's spouse was a senior U.S. government official.

15. In particular, defendant requested that co-conspirator CRACKA gain unauthorized access to accounts belonging to Victim 3's spouse. On or about December 10,

2015, during a Jabber chat, defendant stated to co-conspirator CRACKA, "yo fuck [Victim 3's spouse.] She talks mad shit abt snowden." Defendant continued, "if you come across anything related to [Victim 3's spouse] let me know," and "she needs to getrekt." CRACKA responded, "sure," and told defendant, "i'll see what i can do ;P" Defendant further stated, "if u find her cell or home number omg gimme," explaining that defendant's pseudonymous persona "Bashtien" "want[ed] to phonebomb the shitt outta [Victim 3's spouse]." Later in the conversation, defendant reiterated, "i wish had [Victim 3's spouse's cell]," to which CRACKA responded, "i'll get it soon."

16. In response to defendant's request to target Victim 3's spouse, on or about December 10, 2015, CRACKA obtained the cellphone number of Victim 3's spouse and used social engineering to gain unauthorized access to Victim 3's online account with Verizon.

17. On or about December 12, 2015, defendant asked co-conspirator CRACKA via Jabber whether CRACKA had successfully gained access to Victim 3's Verizon account. CRACKA responded that he was attempting to access Victim 3's account but was having difficulty, and he asked defendant whether defendant wanted to try logging into the account. Defendant replied, "yes :D" Defendant then used login credentials that he received from CRACKA to make multiple attempts to gain unauthorized entry into Victim 3's online Verizon account.

18. Later that day, defendant and co-conspirator CRACKA discussed via Jabber how they should use Twitter to taunt Victim 3. Defendant subsequently used his pseudonymous Twitter account to publicly tweet, "dis is @Snowden, I heard u talkin shit @[Twitter account associated with Victim 3's spouse] so i tok ur acc bish!" With this tweet defendant attached an

image of the sign-in page for Victim 3's Verizon account that the conspirators had altered to include the phrase "cracka_d3f4ult_bashtien_2015."

19. On or about December 12, 2015, co-conspirator CRACKA informed defendant on Jabber that he had obtained the cellphone number and residential phone number associated with Victim 3's Verizon account. Defendant asked CRACKA to call the cellphone number to confirm that it belonged to Victim 3. Defendant also placed a call to Victim 3's residential phone number. Over the next few days, CRACKA called Victim 3's spouse's cellphone and home phone multiple times, with the intent to harass her.

Victim 4

20. In or around December 2015, defendant and other co-conspirators agreed to target Victim 4 in their hacking and phone-harassment scheme. At the time, Victim 4 was a senior U.S. government official who worked for a federal law enforcement agency, and who resided in the Eastern District of Virginia.

21. Specifically, on or about December 18, 2015, co-conspirator CRACKA sent defendant via Jabber a link to a news article about Victim 4, and stated, "[Victim 4's] getting hacked." Defendant responded, "fuck yeah plz do," and stated, "i bet [Victim 4] got some sekretsss." CRACKA replied, "i'll see what i can do :3." Later in the conversation, defendant asked CRACKA whether he'd uncovered Victim 4's cellphone number, stating: "id loooove to phonebomb [Victim 4's] voicemail … and sms spam." Later, defendant stated about Victim 4, "time to fuck her up."

22. On or about December 19, 2015, co-conspirator CRACKA informed defendant over Jabber that he had gained access to Victim 4's online Comcast account. Defendant responded, "roger that, set off the explosivees." CRACKA also informed defendant that he had

accessed Victim 4's home call logs, a copy of which defendant requested. Over the next few hours, defendant and CRACKA discussed different ways they could harass Victim 4 using the information they had unlawfully obtained from Victim 4's Comcast account. CRACKA altered the Comcast account settings for Victim 4's home in the Eastern District of Virginia by, among other things, resetting Victim 4's account password, resetting the passcode to Victim 4's voicemail, causing certain movies to play on the cable box at Victim 4's house, and renaming Victim 4's cable boxes "[Victim 4] is a slut," "fuck the cia," "fuck the fbi," and "fuck you." On or about December 19, 2015, Victim 4 received at least one harassing phone call from the conspirators.

23. On or about December 24, 2015, co-conspirator CRACKA uploaded Victim 4's home telephone call logs to a publicly accessible website and linked to the site from his Twitter account.

Victim 5 and Victim 5's spouse

24. In or around December 2015 and January 2016, defendant and other co-conspirators agreed to target Victim 5 in their hacking and phone-harassment scheme. At the time, Victim 5 was the CEO of a company with an office in the Eastern District of Virginia that provided, among other things, information technology services to government and private sector customers. The conspiracy targeted Victim 5 because Victim 5's company had a business relationship with the federal government.

25. Specifically, on or about December 27, 2015, co-conspirator CRACKA informed defendant via Jabber that he had gained unauthorized access to a Facebook account belonging to Victim 5's spouse. Defendant and CRACKA then discussed ways to harass Victim 5, and CRACKA defaced the Facebook account belonging to Victim 5's spouse. Using the

compromised Facebook account, defendant and CRACKA staged a conversation on Facebook between defendant and Victim 5's spouse, and on or about January 8, 2016, defendant posted screenshots of this supposed conversation online. Also on December 27, 2015, CRACKA gained unauthorized access to a social media account belonging to Victim 5 and defaced it. Later that day, defendant used his pseudonymous Twitter account to tweet: "watching my ninja @[CRACKA's Twitter account] destroy [Victim 5's company] #CWA."

Other Victims

26. In or around January 2016, defendant encouraged co-conspirator CRACKA to execute a swatting campaign against the Palm Beach County Sheriff's Office in Florida. Specifically, on or about January 16, 2016, defendant and co-conspirator CRACKA engaged in the following Jabber conversation:

SENDER	TIME	TEXT
CRACKA	3:46:11 PM	im gonna swat a police department
CRACKA	3:47:03 PM	yolo
CRACKA	3:47:04 PM	lmao
CRACKA	3:48:49 PM	what shall i say
Defendant	**3:49:10 PM**	**ayyyyyyyy yolo fuck it**
CRACKA	3:49:23 PM	what shall i say tho
Defendant	**3:49:31 PM**	**hopefully they will have a shootout and kill eachother**
CRACKA	3:49:32 PM	i got bombs in the building?
CRACKA	3:49:36 PM	LOL yeee
CRACKA	3:49:49 PM	shall i say i got bombs in the building?
Defendant	**3:51:25 PM**	**yeaaa that usually works**
Defendant	**3:51:33 PM**	**nano thermite hhhhhhhh**
CRACKA	3:51:54 PM	LOL aight im doing it now
CRACKA	3:52:14 PM	im nervous as fuck
CRACKA	3:54:08 PM	IM DOING IT

27. After engaging in the above conversation with defendant, CRACKA called the Palm Beach County Sheriff's Office and falsely claimed that there were bombs located in the Office's Belle Glade administrative building, resulting in that building's evacuation and the

deployment of a specialty bomb squad. Shortly after making the swatting call, CRACKA wrote to defendant on Jabber: "i told them i had bombs at their building," and "they asked me where i put them and i said i dont know." Defendant replied, "imagine all the ppl running around rn [right now]. thinking there is a bomb in the building." CRACKA wrote back, "hhahahaa. 'I GOT KIDS.'" As defendant and CRACKA exchanged online links to the unfolding press coverage of the hoax bomb-threat call, defendant wrote to CRACKA, "they skuuuuurdd" and "viva la revolution."

28. In or around January 2016, defendant falsely claimed on his pseudonymous Twitter account that he had successfully compromised computer systems belonging to the government agency NASA. In particular, from in or about January 28 to in or about January 31, 2016, defendant used the Twitter account @OPNASADRONES – which he created and controlled – to claim that he had gained unauthorized access to sensitive NASA information. Defendant uploaded this purportedly "leaked" data – including hundreds of aircraft and radar videos, thousands of flight logs, and data on thousands of NASA employees – to a publicly accessible website. This "leaked" data was in fact either fake or publicly available. NASA incurred a significant pecuniary loss in investigating defendant's false computer intrusion claims.

* * *

29. This Statement of Facts includes those facts necessary to support the plea agreement between the defendant and the United States. It does not include each and every fact known to the defendant or to the United States, and it is not intended to be a full enumeration of all of the facts surrounding the defendant's case.

30. The actions of the defendant, as recounted above, were in all respects knowing and deliberate, and were not committed by mistake, accident, or other innocent reason.

31. If the defendant breaches the plea agreement, then pursuant to the plea agreement, he waives any rights under Federal Rule of Criminal Procedure 11(f), Federal Rule of Evidence 410, the United States Constitution, and any federal statute or rule in objecting to the admissibility of the statement of facts in any such proceeding.

Respectfully submitted,

Dana J. Boente
United States Attorney

By: _____
Maya D. Song
Jay V. Prabhu
Assistant United States Attorneys

Joseph V. Longobardo
Special Assistant United States Attorney (LT)

Defendant's signature: After consulting with my attorneys and pursuant to the plea agreement entered into this day between the defendant, JUSTIN GRAY LIVERMAN, and the United States, I hereby stipulate that the above Statement of Facts is true and accurate, and that had the matter proceeded to trial, the United States would have proved the same beyond a reasonable doubt.

Date: 12/27/16

JUSTIN GRAY LIVERMAN
Defendant

Defense counsel signature: I am the defendant's attorney. I have carefully reviewed the above Statement of Facts with him. To my knowledge, his decision to stipulate to these facts is an informed and voluntary one.

Date: 1/6/17

Marina Medvin, Esq.
Tor Ekeland, Esq.
Jay Leiderman, Esq.
Counsel for the Defendant